Evenly distributed unitaries: on the structure of unitary designs

D. Gross, K. Audenaert, and J. Eisert
Institute for Mathematical Sciences, Imperial College London, Princes Gate, London SW7 2PE, UK and
QOLS, Blackett Laboratory, Imperial College London, Prince Consort Road, London SW7 2BW, UK *
(Dated: February 1, 2008)

We clarify the mathematical structure underlying *unitary t-designs*. These are sets of unitary matrices, evenly distributed in the sense that the average of any t-th order polynomial over the design equals the average over the entire unitary group. We present a simple necessary and sufficient criterion for deciding if a set of matrices constitutes a design. Lower bounds for the number of elements of 2-designs are derived. We show how to turn mutually unbiased bases into approximate 2-designs whose cardinality is optimal in leading order. Designs of higher order are discussed and an example of a unitary 5-design is presented. We comment on the relation between unitary and spherical designs and outline methods for finding designs numerically or by searching character tables of finite groups. Further, we sketch connections to problems in linear optics and questions regarding typical entanglement.

I. INTRODUCTION

Before introducing the notion of a unitary design it is worthwhile to look at the analogue structure on spheres in $\mathbb{R}^n$. Imagine one is interested in the average value of a real function f defined on an n-dimensional real sphere $\mathcal{S}^n$. That value might be hard to compute in general so it could be sensible to estimate it by averaging over a finite set of unit vectors $\mathcal{D} = \{|\psi_1\rangle, \ldots, |\psi_K\rangle\}$. Of course, for any such finite set, there are functions whose true average value deviates arbitrarily much from the one approximated by summing over $\mathcal{D}$; but the more points the test set includes and the more "even" these vectors are distributed, the more "exotic" such functions have to be. The following notion aims to quantitatively capture the quality of a set of points for these purposes: a finite subset $\mathcal{D}$ of S^n is called a *spherical t-design* if the average of every t-th order polynomial p over $\mathcal{S}^n$ equals p's average taken over $\mathcal{D}$. A large body of literature has been devoted to the construction and exploration of designs. Many of the relevant references can be found in the accessible article Ref. [3].

One can adapt the definition of spherical designs to complex vector spaces (simply by substituting the real sphere by the set of complex unit vectors) with obvious applications in quantum mechanics. In the context of quantum information theory, 2-designs appeared in Refs. [4, 5, 6, 7, 8, 9], to name a few. Two prominent examples of complex spherical 2-designs are here known by the names of *mutually unbiased bases* [3, 8, 10] and *symmetric informationally complete POVMs* [3, 5, 8] respectively.

Quite recently, Dankert et al. introduced the notion of a *unitary t-design* by replacing the real sphere $\mathcal{S}^n$ by the set of unitary matrices $U(d)$ in the definition of spherical designs [1, 2]. Averages are here to be taken with respect to the Haar measure. In the sense made precise above, the theory of unitary designs thus aims to identify finite nets of unitaries, which cover the entire group as tightly as possible.

Such nets are interesting for various reasons. Abstractly, unitary designs can serve as testbeds for examining conjectures concerning the unitary group: their even distribution here means that they "cover many complementary aspects" of $U(d)$. Also, spherical designs naturally appear in optimal solutions to several physical problems, ranging from quantum state tomography and optimal estimation using finite ensembles to quantum key distribution [5, 6, 7, 11] – it is sensible to assume that similar applications for their unitary counterpart can be found. More concretely, unitary designs have been applied to quantum process estimation and fidelity estimation of channels using random states [1, 2]; quantum cryptography [12] and data hiding protocols [13]. Naturally, designs can be used to estimate Haar averages using classical computers. For the case of averages of polynomial functions, the results are guaranteed to be correct (there are, however, other methods for tackling this specific problem; see Appendix VIII A and Ref. [14]). For non-polynomial functions one obtains at least an educated guess. Going beyond finite-dimensional quantum systems, Haar averages over $U(d)$ appear in the context of energy-preserving transformations of d bosonic modes. Such transformations are notably relevant as passive linear optical transformations of states of light modes [15, 16]. Lastly, we believe the problem to be of inherent geometrical interest.

As most of the present work is concerned with unitary 2-designs, we now state the precise definition for this special case (see, however, Section V A):

Definition 1 (Unitary design [1, 2])**.** *A set $\mathcal{D} = \{U_k\}_{k=1,\ldots,K}$ of unitary matrices on $\mathcal{H} = \mathbb{C}^d$ is a* unitary 2-design *if it fulfills the equivalent conditions:*

1. (Averages) *Let p be a polynomial in $2d^2$ variables. We can conceive p as a function on $U(d)$ by evaluating it on the matrix elements and their complex conjugates of a given matrix: $p(U) := p(U^i{}_j, \bar{U}^i{}_j)$. One now demands that for any p which is homogeneous of degree two in each variable, the relation*

$$\frac{1}{K}\sum_{U_k\in\mathcal{D}} p(U_k) = \int_{U(d)} p(U)dU \qquad (1)$$

be fulfilled.

*Electronic address: david.gross@imperial.ac.uk

2. (Twirling of states) *For all* $\rho \in \mathcal{B}(\mathcal{H} \otimes \mathcal{H})$

$$\frac{1}{K} \sum_{U_k \in \mathcal{D}} (U_k \otimes U_k)\, \rho\, (U_k \otimes U_k)^\dagger \tag{2}$$

$$= \int_{U(d)} (U \otimes U)\, \rho\, (U \otimes U)^\dagger dU. \tag{3}$$

3. (Twirling of channels) *For any quantum channel* Λ

$$\frac{1}{K} \sum_{U_k \in \mathcal{D}} U_k^\dagger \Lambda(U_k \rho U_k^\dagger) U_k \tag{4}$$

$$= \int_{U(d)} U^\dagger \Lambda(U \rho U^\dagger) U dU.$$

The problem has a long history, which is formulated mostly in the second of the three equivalent guises listed above. The "twirling" operation originates from invariant theory (where it is sometimes called "transfer homomorphism") and has, to our knowledge, first been introduced to quantum information theory in Ref. [17], giving rise to the concept of a "Werner state". Later, it was noted that in $d = 2$ (i.e., for single qubits), it suffices to average over a finite set of unitaries [18]. A construction for general dimensions – employing non-evenly weighted unitaries – appeared in Ref. [19]. DiVincenzo et al. [13] realized that the *Clifford group* [20, 23] for qubit systems exhibits the property given in Eq. (2); a fact which was later generalized to systems of prime-power dimensions by Chau [12]. Similar ideas appeared in Ref. [21]. A first concise treatment was given in a master thesis by Dankert [1] (where the term of a *unitary* t*-design* has been coined) and in a later paper by Dankert et al. [2]. In these publications, the equivalence of the criteria in Definition 1 has been made explicit and the question of how to efficiently implement the unitaries of certain designs was addressed.

Despite the large amount of interest paid to the problem, the following natural questions have been left open and will partly be answered in this paper:

1. *In which dimensions do unitary* 2*-designs exist and when can they be explicitly constructed?* While we do not have a general answer to this question, a host of examples is provided in Sections III and IV C. [Note added in revised version: After this article had been submitted, A. Scott made us aware of Ref. [45]. This extremely general paper proves – among other things – the existence of unitary designs for every t and d (it does not provide an explicitly way for constructing the designs). Thus, the question posed above can partly be answered affirmatively.]

2. *What is the minimal number of elements needed for a* 2*-design?* See Section II C for a lower bound, which we conjecture to be tight in leading order.

3. *Is there an easy criterion to decide whether a given set of matrices constitutes a design?* This question is answered affirmatively in Section II B. We transfer the concept of a *frame potential* [3, 31] from spherical to unitary designs. The frame potential is a simple polynomial expression in the matrix elements, which is minimized exactly for designs. This criterion even allows for numerical searches in spaces of small dimensions.

4. *Can one find designs among matrix groups?* Section III treats this special case. It turns out that the theory is especially clear when one restricts attention to groups. The frame potential will be re-interpreted in terms of basic character theory.

5. *Is it possible to explicitly construct approximate unitary designs?* In Section IV B we give an explicit construction for turning mutually unbiased bases (MUBs) into unitary matrices which asymptotically approximate 2-designs. More precisely, the prescription yields a set of unitaries for every prime-power dimension d. These sets approximate 2-designs as $d \to \infty$. Also, the cardinality of such *asymptotic designs* is of the same order as the lower bound derived earlier.

6. The set of operators $\mathcal{B}(\mathbb{C}^d)$ on $\mathbb{C}^d$ form a d^2-dimensional Hilbert space. *What is the connection between the unitary designs in* $U(d)$ *and spherical designs in* $\mathbb{C}^{d^2}$*?* The relation can be made rather explicit in terms of the Jamiołkowski isomorphism and the frame potential. Both spherical and unitary designs correspond to minima of the potential – yet under different constraints. This statement is made precise in Section II B.

7. *What about more general concepts such as* t*-designs for* $t > 2$ *or substituting* $U(d)$ *by other groups?* We will discuss this general scenario in Section V A and present an example of a qubit 5-design.

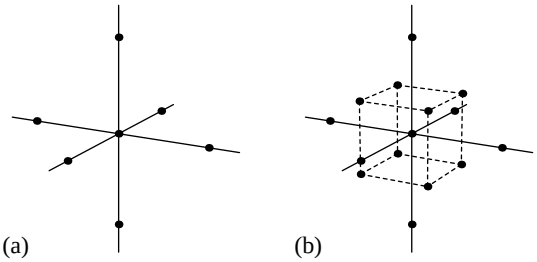

FIG. 1: Visualization of the 12-element Clifford 2-design described in Section IV C. As up to phases $SU(2) \simeq SO(3)$, every qubit unitary corresponds to a three-dimensional rotation. The group $SO(3)$, in turn, can be pictured as a ball with radius π, where antipodes on the boundary are identified. This is done by associating to every rotation by an angle $\phi \in [0, \pi]$ about the unit-vector $\hat{n}$ the point $\phi\, \hat{n} \in \mathbb{R}^3$. Figure (a) shows the four Pauli matrices $\mathbb{1}, \sigma_x, \sigma_y, \sigma_z$ in this representation. The non-trivial Pauli operations lie on the boundary of the ball and hence appear twice: σ_x, e.g., at $\pm(\pi, 0, 0)^T$. Adding eight further Clifford operations, which correspond to the vertices $2\pi/\sqrt{27}(\pm 1, \pm 1, \pm 1)^T$ of a cube, we arrive at the 2-design pictured in Figure (b).

II. GENERAL THEORY

A. Preliminaries

In this section we are going to derive a simple criterion for identifying 2-designs as well as lower bounds for the number of elements K they need to contain. Before stating these results, let us shortly recall some general facts about *twirling channels* and *completely positive maps* which will be needed in the sequel.

Let $\{U_g\}_{g\in G}$ be a unitary representation of some group G on a Hilbert space $\mathcal{H}$. The *twirling channel* induced by G and the representation U_g is

$$T(A) = \int_g U_g A U_g^\dagger \, dg, \tag{5}$$

where dg stands for the Haar measure of the group G. Denote the projection operators onto the irreducible subspaces of $\{U_g\}_g$ by $\{P_i\}_i$. For simplicity we assume that the representation is a direct sum of *inequivalent* irreducible ones (see Appendix VIII A for the general case). By Schur's Lemma $T(A) = A$ if and only if A is a linear combination of the P_i's. Indeed, setting $P_i' := P_i/\mathrm{tr}\, P_i$, one easily checks that

$$T(A) = \sum_i \mathrm{tr}(P_i' A) P_i. \tag{6}$$

Setting $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$, $G = U(d)$ represented as $U \mapsto U \otimes U$, we arrive at the UU*-twirling* channel T_{UU} defined in Eq. (3), which has played a prominent role in quantum information theory. In order to identify the irreducible subspaces, define the *flip operator* $\mathbb{F}$ which acts by permuting the tensor factors: $\mathbb{F}|i\rangle \otimes |j\rangle = |j\rangle \otimes |i\rangle$. Its eigenspaces are the sets of *symmetric* and *anti-symmetric* vectors respectively. The projection operators onto these spaces will be denoted by $P_S = (\mathbb{1} + \mathbb{F})/2$ and $P_A = (\mathbb{1} - \mathbb{F})/2$. We have that $\dim P_S = d(d+1)/2$ and $\dim P_A = d(d-1)/2$.

Moving on, we recall the well-known correspondence between completely positive maps (*cp maps*) sending $\mathcal{B}(\mathbb{C}^d) \to \mathcal{B}(\mathbb{C}^d)$ and states on $\mathbb{C}^d \otimes \mathbb{C}^d$. Let Λ be such a map. Choose a basis $\{|i\rangle\}_i$ in $\mathbb{C}^d$ and let $|\Psi\rangle := \sum_i^d |i\rangle \otimes |i\rangle$ be an (unnormalized) maximally entangled vector in $\mathbb{C}^d \otimes \mathbb{C}^d$. The object

$$C_\Lambda := (\mathbb{1} \otimes \Lambda)|\Psi\rangle\langle\Psi| = \sum_{i,j} |i\rangle\langle j| \otimes \Lambda(|i\rangle\langle j|) \tag{7}$$

is called the *Choi matrix* of Λ. It is also known as the *process matrix* and the correspondence in Eq. (7) goes by the name of *Jamiołkowski isomorphism*. The name is justified as $\Lambda \mapsto C_\Lambda$ is invertible:

$$\Lambda(|i\rangle\langle j|) = \langle i|_1 \, C_\Lambda \, |j\rangle_1. \tag{8}$$

In what follows, we will write $T_\mathcal{D}$ for the channel induced by a set of unitaries $\mathcal{D}$ via Eq. (2) and denote the corresponding Choi matrix by $C_\mathcal{D}$. Likewise, C_{UU} designates the Choi matrix of T_{UU}.

B. The frame potential

The various $\forall$-quantifiers in Definition 1 make it hard to identify a given set of matrices as a design. Any exploration of this structure would thus greatly benefit from a simple criterion for the property of "being a design". Indeed, for the case of spherical designs such a tool is well-known (see Ref. [3] and references therein): a set of vectors $\{|\psi_1\rangle, \ldots, |\psi_K\rangle\}$ is a spherical 2-design in $\mathbb{C}^d$ if and only if

$$\sum_{k,k'} |\langle\psi_k|\psi_{k'}\rangle|^4 / K^2 = 2/(d^4 + d^2). \tag{9}$$

The expression on the left-hand side has been linked in Ref. [5] to a concept which appeared in the context of *frame theory* in an equally insightful and enjoyable paper by Benedetto and Fickus [31]. The authors considered a physical model to introduce a notion of "evenly distributed" vectors: if we assume that K particles on the unit-sphere with respective coordinates $|\psi_k\rangle$ are subject to a repulsive force proportional to $\langle\psi_k|\psi_{k'}\rangle^2$, then the left-hand-side of Eq. (9) gives the *potential* of the configuration. Consequently, the quantity is referred to as the (spherical) *frame potential* [46]. It turns out that $2/(d^4+d^2)$ is the lowest value the frame potential can possibly attain and so there is a one-one correspondence between global minimizers of the frame energy and spherical 2-designs.

Our first result transfers this nice concept to the setting of unitary designs.

Theorem 2 (Frame potential)**.** *Let $\mathcal{D} = \{U_k\}_{k=1,\ldots,K}$ be a set of unitaries. Define the* frame potential *of $\mathcal{D}$ to be*

$$\mathcal{P}(\mathcal{D}) = \sum_{U_k, U_{k'} \in \mathcal{D}} |\,\mathrm{tr}\, U_k^\dagger U_{k'}|^4 / K^2. \tag{10}$$

The set $\mathcal{D}$ is a unitary 2-design if and only if $\mathcal{P}(\mathcal{D}) = 2$, which is a lower bound to the global minimum of the potential.

Theorem 2 allows us to discuss the connection between unitary and spherical designs quite explicitly. Recall that the *Hilbert-Schmidt inner product* on $\mathcal{B}(\mathbb{C}^d)$ is defined as $\langle A|B\rangle_{HS} := \mathrm{tr}(A^\dagger B)/d$. In the spirit of the Jamiołkowski map, we can establish an isomorphism between $\mathcal{B}(\mathbb{C}^d)$ as a vector space and $\mathbb{C}^d \otimes \mathbb{C}^d$. Explicitly, we map U to $|v_U\rangle$ where

$$v_U^{ij} = U^i{}_j / \sqrt{d}. \tag{11}$$

Here, we have used the notation $v^{ij} = (\langle i| \otimes \langle j|)\,|v\rangle$ and $U^i{}_j = \langle i|U|j\rangle$ for the respective matrix elements [47]. One checks that $|v_U\rangle$ is a normalized maximally entangled vector if and only if U is unitary. Hence, we can re-phrase Theorem 2 as: $\mathcal{D}$ is a unitary 2-design if and only if

$$\sum_{U_k, U_{k'} \in \mathcal{D}} |\langle v_{U_k}|v_{U_{k'}}\rangle|^4 / K^2 = 2/d^4, \tag{12}$$

which is the global minimum of the spherical frame potential for K *maximally entangled* vectors. Note the close similarity to Eq. (9).

The relation between unitary designs in $U(d)$ and spherical designs in $\mathbb{C}^d \otimes \mathbb{C}^d$ now becomes apparent: both correspond to minima of the frame potential, yet under different constraints. For spherical designs the minimum is taken in the set of all normalized vectors; whereas in the unitary case one demands that the vectors are also maximally entangled.

Theorem 2 also facilitates numerical searches for designs on low dimensional spaces. Indeed, the authors have written a program for the MatLab computer system, which numerically minimizes the frame potential of a set of operators on $\mathbb{C}^2$. If the set has $K \geq 12$ elements, a multitude of unitary 2-designs is found, while there seem to be no solutions for $K < 12$. These findings support Conjecture 4.

Proof. (of Theorem 2) Using the notation introduced in Section II A, let $\Delta := C_{\mathcal{D}} - C_{UU}$. Obviously, $\mathcal{D}$ is a 2-design if and only if $||\Delta||_2^2 := \operatorname{tr}|\Delta|^2 = 0$. We compute

$$\operatorname{tr}(\Delta^\dagger \Delta) = \operatorname{tr}(C_{UU}^\dagger C_{UU} - C_{UU}^\dagger C_{\mathcal{D}} - C_{\mathcal{D}}^\dagger C_{UU} + C_{\mathcal{D}}^\dagger C_{\mathcal{D}})$$

and treat the terms in turn. To that end introduce a basis $\{|i\rangle\}$ in $\mathbb{C}^d \otimes \mathbb{C}^d$ such that the first $d_s := \dim P_S = d(d+1)/2$ vectors are symmetric and the last $d_a := \dim P_A = d(d-1)/2$ ones anti-symmetric with respect to $\mathbb{F}$. In the formulas below, we will sometimes write $|i_S\rangle$ or $|i_A\rangle$ to indicate the subset a given vector belongs to. Note that the vector $|\Psi\rangle$ introduced in Section II A can be written as $|\Psi\rangle = \sum_{i_s} |i_S\rangle \otimes |i_S\rangle + \sum_{i_A} |i_A\rangle \otimes |i_A\rangle$. One then finds

$$\begin{aligned} C_{UU} &= \sum_{i_S, j_S} |i_S\rangle\langle j_S| \otimes \operatorname{tr}(|i_S\rangle\langle j_S| P_S) P'_S + S \leftrightarrow A \\ &= P_A \otimes P'_A + P_S \otimes P'_S. \end{aligned}$$

We have used the abbreviation $S \leftrightarrow A$ to denote the term which follows from the preceding one by a straight-forward substitution of symmetric by anti-symmetric expressions, and as before $P'_S = P_S / \operatorname{tr} P_S$, $P'_A = P_A / \operatorname{tr} P_A$. Further:

$$C_{\mathcal{D}} = \sum_{i,j} |i\rangle\langle j| \otimes \left(\sum_k U_k^{\otimes 2} |i\rangle\langle j| (U_k^\dagger)^{\otimes 2} / K \right).$$

Hence,

$$\operatorname{tr}(C_{UU}^\dagger C_{UU}) = d_S^{-2} \operatorname{tr}(P_S \otimes P_S) + d_A^{-2} \operatorname{tr}(P_A \otimes P_A) = 2$$

and

$$\begin{aligned} &\operatorname{tr}(C_{UU}^\dagger C_{\mathcal{D}}) \\ &= K^{-1} \sum_{i,j} \operatorname{tr}(P_S |i\rangle\langle j|) \operatorname{tr}\left(P'_S \sum_k U_k^{\otimes 2} |i\rangle\langle j| (U_k^\dagger)^{\otimes 2} \right) \\ &\quad + S \leftrightarrow A \\ &= K^{-1} \sum_{i_S} \operatorname{tr}\left(\sum_k U_k^{\otimes 2} P'_S |i_S\rangle\langle i_S| (U_k^\dagger)^{\otimes 2} \right) + S \leftrightarrow A \\ &= \sum_{i_S} \operatorname{tr}(P'_S |i_S\rangle\langle i_S|) + S \leftrightarrow A \\ &= 2 = \operatorname{tr}(C_{\mathcal{D}}^\dagger C_{UU}). \end{aligned}$$

Lastly:

$$\begin{aligned} &\operatorname{tr}(C_{\mathcal{D}}^\dagger C_{\mathcal{D}}) \\ &= K^{-2} \sum_{i,j} \sum_{k,k'} \operatorname{tr}\left(U_k^{\otimes 2} |j\rangle\langle i| (U_k^\dagger)^{\otimes 2} \; U_{k'}^{\otimes 2} |i\rangle\langle j| (U_{k'}^\dagger)^{\otimes 2} \right) \\ &= K^{-2} \sum_{k,k'} |\operatorname{tr} U_k^\dagger U_{k'}|^4 = \mathcal{P}(D). \end{aligned}$$

The claim is now immediate. □

For the construction of approximate unitary designs in Section IV B, we record the following corollary.

Corollary 3. *Let $\mathcal{D}$ be a set of unitary matrices, C_{UU} and $C_{\mathcal{D}}$ as defined in Section II A. Then*

$$||C_{UU} - C_{\mathcal{D}}||_2^2 = \mathcal{P}(\mathcal{D}) - 2.$$

C. A lower bound

Intuitively it is clear that constructing unitary designs becomes more challenging the fewer elements K one allows for (c.f. Theorem 6.6). This section is devoted to finding a lower bound for K as a function of the dimension d.

What is the situation to date? Before the present paper, all known families of 2-designs were subgroups of the Clifford group $\mathcal{C}_d$ in prime-power dimensions d. In the context of quantum information, the Clifford group is the set of unitaries mapping the set of Weyl operators (also known as: generalized Pauli operators) to itself under conjugation [20]. An introduction into this theory will be given in Section IV C, where all claims made in this paragraph will be elaborated on. References [1, 2, 13, 21] use the fact that the full Clifford group $\mathcal{C}_d$ constitutes a 2-design. However, as the cardinality of $\mathcal{C}_d$ grows exponentially in d (c.f. Eq. (50)), one might hope for the existence of more optimal designs. Fortunately, in Ref. [12] it has been realized that a particular subgroup of the Clifford group already possesses the 2-design property. The group's order scales as $O(d^5)$. What is more, the existence of Clifford 2-designs with $d^2(d^2-1) = O(d^4)$ elements has been established for several dimensions [12]. As will be explained in Section IV C, $d^2(d^2-1)$ is in fact the smallest value a design based on the Clifford group can possibly have and that value will subsequently be referred to as the *Clifford bound*. For various reasons to be explained later, we believe this to be a general lower bound for the cardinality of any 2-design, even for constructions which are not based on the Clifford group.

Conjecture 4. *The Clifford bound*

$$d^4 - d^2 \tag{13}$$

is a lower bound for the cardinality of any unitary 2-design.

While we were not able to prove this conjecture, an estimate which equals the Clifford bound in leading order is established below.

Theorem 5 (Lower bound on K)**.** *A unitary 2-design in dimension d has no fewer than*

$$d^4 - 2d^2 + 2 \tag{14}$$

elements.

Note that a spherical 2-design in $\mathbb{C}^d \otimes \mathbb{C}^d$ has at least d^4 elements – so the slightly higher frame potential characteristic for unitary 2-designs might allow one to save a few elements as compared to spherical 2-designs.

Proof. We follow an idea from Ref. [5]. Let $|v_U\rangle := U \otimes \mathbb{1} |v_0\rangle$ for some maximally entangled vector $|v_0\rangle$. Define a homogeneous polynomial p of degree $2, 2$ in U by

$$p(U) := \langle v_U|A|v_U\rangle \operatorname{tr}(|v_U\rangle\langle v_U| B). \tag{15}$$

Certainly, Eq. (1) holds and hence, as A and B are arbitrary, the relation

$$\begin{aligned} &\sum_{U\in\mathcal{D}} \langle v_U|A|v_U\rangle \, |v_U\rangle\langle v_U|/K \qquad (16)\\ = &\int \langle v_U|A|v_U\rangle \, |v_U\rangle\langle v_U| \, dU =: \Lambda(A) \end{aligned}$$

must hold and defines a channel $A \mapsto \Lambda(A)$. We want to compute the kernel of Λ.

The channel Λ is clearly $U \otimes \mathbb{1}$-covariant:

$$\Lambda((U \otimes \mathbb{1})A(U \otimes \mathbb{1})^\dagger) = (U \otimes \mathbb{1}) \, \Lambda(A) \, (U \otimes \mathbb{1})^\dagger. \tag{17}$$

But because for any maximally entangled state $(\mathbb{1} \otimes V)|v\rangle = (V' \otimes \mathbb{1})|v\rangle$ for some V', Λ is also $\mathbb{1} \otimes V$ and hence even $U \otimes V$-covariant, for all unitaries U, V. Invoking Schur's Lemma one concludes that Λ must be a mixture of projections onto the $U \otimes V$-invariant subspaces of $\mathcal{B}(\mathcal{H})$. What are these spaces? Let us first identify the irreducible components of $U \cdot U^\dagger$. The multiples of the identity (M_1 for short) clearly form an irreducible component by themselves. Its complement is the space of trace-less operators (M_2). Now, $U \cdot U^\dagger$ must act irreducibly on M_2, because there exists bases of mutually conjugate trace-less operators [48].

Surely then, $M_1 \otimes M_1$ (multiples of the identity), $M_1 \otimes M_2, M_2 \otimes M_1$ (the local observables of the form $\mathbb{1} \otimes X, X \otimes \mathbb{1}$) and $M_2 \otimes M_2$ are invariant under $U \otimes V \cdot U^\dagger \otimes V^\dagger$. A moment of thought reveals that they are irreducible (think of cyclic vectors). Clearly, $M_1 \otimes M_1$ has no non-trivial intersection with $\ker(\Lambda)$, while $M_1 \otimes M_2, M_2 \otimes M_1 \subset \ker(\Lambda)$. What about $M_2 \otimes M_2$? Because of Λ's structure, either any element of $M_2 \otimes M_2$ is in the kernel or else, none is. Setting $B = A^\dagger$ and evaluating Eq. (15) we see that

$$p(U) = |\langle v_U|A|v_U\rangle|^2 \geq 0, \tag{18}$$

so $\Lambda(A) = 0$ if and only if $\langle v|A|v\rangle = 0$ for all maximally entangled vectors $|v\rangle$. To conclude that $M_2 \otimes M_2$ has no intersection with $\ker \Lambda$, we only need to assure the existence of a single traceless observable X and a single maximally entangled state $|v\rangle$ such that $\langle v|X \otimes X|v\rangle \neq 0$, which is trivially possible. Hence $\operatorname{rank} \Lambda = d^4 - \dim \ker \Lambda = d^4 - \dim(M_1 \otimes M_2) - \dim(M_2 \otimes M_1) = d^4 - 2(d^2 - 1)$. But the rank of Λ cannot be larger than K, by Eq. (16). □

III. GROUP DESIGNS

When searching for unitary designs, it might prove helpful to assume some additional structure in order to narrow down the search space and simplify the proofs. Indeed, sets of unitary matrices appear most naturally as representations of finite groups and (except for our numerical findings), all known designs are matrix groups. It will turn out that the concept of unitary designs has a very natural interpretation in terms of representation theory.

A. Irreducible constituents

We will be concerned with sets $\mathcal{D}$ of unitaries which form a finite matrix group on $\mathbb{C}^d$. It will prove convenient to conceive $\mathcal{D}$ as the image of a representation $U : g \mapsto U_g$ of some finite group G. Recalling the notions of Section II A, it is clear that the channel $T_\mathcal{D}$ is nothing but the twirling channel associated with the representation U. By Eq. (5), $T_\mathcal{D}$ will project onto the irreducible subspaces of this representation. As any operator of the form $U_g \otimes U_g$ commutes with the flip operator $\mathbb{F}$, we know that the symmetric and anti-symmetric subspaces of $\mathbb{C}^d \otimes \mathbb{C}^d$ will be among the invariant subspaces of $\{U_g \otimes U_g \,|\, g \in G\}$. In general, these spaces are not going to be irreducible. We now see what makes representations U which induce a 2-design special: $T_\mathcal{D} = T_{UU}$ *(and hence $\mathcal{D}$ is a design) if and only if the representation $g \mapsto U_g \otimes U_g$ has exactly two irreducible components.*

Simple as this observation may be, it must not be underestimated: it allows us to understand designs from a group theoretical point of view. The next section will further elaborate on this approach.

B. Characters

Let us devote one paragraph to recall some very basic notions and results from representation theory [29]. To every unitary representation $U : g \mapsto U_g$ of a finite group, one associates its *character* $\zeta(g) = \operatorname{tr} U_g$. One says that the representation *affords* ζ. Denote the irreducible representations (*irreps*) of G by $\{V^{(i)}\}_i$ and their associated *irreducible characters* by $\{\chi_i\}$. One introduces a scalar product between characters by setting

$$\langle \zeta, \chi \rangle := |G|^{-1} \sum_g \bar{\zeta}(g)\chi(g). \tag{19}$$

It is a well-known and fundamental relation that the irreducible characters are ortho-normal: $\langle \chi_i, \chi_j \rangle = \delta_{i,j}$. The fact that any representation reduces to a direct sum of irreps means that any character can be expanded in terms of the irreducible ones and further that $\langle \zeta, \chi_i \rangle$ gives the number of times n_i the i-th irrep occurs in the decomposition of the representation affording ζ. Finally, if $\zeta = \sum_i n_i \chi_i$, then $||\zeta||^2 = \langle \zeta, \zeta \rangle = \sum_i n_i^2$.

Now, let $\mathcal{D}, G, U$ be as in Section III A. We compute the frame potential of $\mathcal{D}$:

$$\begin{aligned}\mathcal{P}(\mathcal{D}) &= \sum_{g,g'} |\operatorname{tr} U_{g^{-1}g'}|^4/|G|^2 \qquad (20)\\ &= \sum_{g} |\operatorname{tr} U_g|^4/|G| \\ &= \sum_{g} \overline{(\operatorname{tr} U_g \otimes U_g)}(\operatorname{tr} U_g \otimes U_g)/|G| \\ &= \langle \zeta_{U^{(2)}}, \zeta_{U^{(2)}} \rangle = ||\zeta_{U^{(2)}}||^2,\end{aligned}$$

where $\zeta_{U^{(2)}}(g) = \operatorname{tr}(U_g \otimes U_g) = \zeta_U(g)^2$ is the character of the representation $U^{(2)} : g \mapsto U_g \otimes U_g$. In other words, the frame potential of a group design is the squared norm of the character of $U^{(2)}$.

We can now rederive Theorem 2. By this section's first paragraph, $||\zeta_{U^{(2)}}||^2 = \sum_i n_i^2$, which equals 2 if and only if $U^{(2)}$ has exactly two irreducible components. This in turn is equivalent to U inducing a 2-design, as has been shown in Section III A. Note how much the group structure simplified the proof.

It seems remarkable that the frame potential offers a very natural interpretation in terms of two completely unrelated structures: from the point of view of frame theory, it is a purely *geometrically* motivated measure for the "eveness" of a distribution. In terms of group representation theory, it seemlessly takes on an *algebraic* role.

C. General results and properties

Consider a group design $\mathcal{D} = \{U_g \,|\, g \in G\}$. The *center* $\mathcal{Z}(U)$ of U are the elements of $\mathcal{D}$ which commute with any U_h. By Schur's Lemma, if U is irreducible, we have that $U_g \in \mathcal{Z}(U) \Leftrightarrow U_g \propto \mathbb{1}$. Now choose one representative of each coset $\mathcal{D}/\mathcal{Z}(U)$ and assemble these unitaries in a set $\mathcal{D}'$ ($\mathcal{D}'$ is called a *transversal* of $\mathcal{D}/\mathcal{Z}(U)$). Using Eq. (2), one sees that D' is a 2-design of cardinality $|\mathcal{D}|/|\mathcal{Z}(U)|$. From now on, we will restrict attention to such reduced sets. Consequently, for any representation U of G, we will define $\mathcal{D}_U$ to be a transversal of $\{U_g \,|\, g \in G\}/\mathcal{Z}(U)$ and refer to $\mathcal{D}_U$ as the *group design induced by* U.

Using this definition, let us collect and extend the results on group designs in the following theorem.

Theorem 6 (Group designs)**.** *Let G be a finite group and U a unitary representation of G on $\mathbb{C}^d$ affording the character ζ. The following are equivalent:*

1. *The set $\mathcal{D}_U$ is a 2-design.*
2. *The representation $U^{(2)} : g \mapsto U_g \otimes U_g$ has no more than two irreducible components.*
3. *It holds that $||\zeta_{U^{(2)}}||^2 = 2$.*
4. *The characters*

$$\begin{aligned}\chi_S(g) &:= (\chi(g)^2 + \chi(g^2))/2,\\ \chi_A(g) &:= (\chi(g)^2 - \chi(g^2))/2\end{aligned}$$

are irreducible.

Further:

5. *The cardinality $K = |\mathcal{D}_U|$ is a multiple of d and $1/2d(d \pm 1)$.*
6. *Let H be a finite group represented on $\mathbb{C}^d$ by V. If $\{V_h \,|\, h \in H\} \supset \{U_g \,|\, g \in G\}$ then $\mathcal{F}(\mathcal{D}_V) \leq \mathcal{F}(\mathcal{D}_U)$.*
7. *The frame potential of a matrix group is an integer.*
8. *A necessary condition for $\mathcal{D}_U$ to be a 2-design is that U is irreducible.*
9. *For $d > 2$, there are no real-valued group representations which form a 2-design.*

Statement 5 can be used in conjunction with Section II C to derive bounds on K. For example, for $d = 2$, it holds that $K \geq 10$ by Theorem 5. But we now know that K must be divisible by 2 and 3, so that $K \geq 12$. As unitary group designs of order 12 in dimension 2 do indeed exist, we know that the bound is tight. Unfortunately, this is the only case where we can make lower and upper bounds match. Note also, that 12 is the value predicted by the Clifford bound for $d = 2$, supporting our conjecture.

The 6-th point says that "supergroups have lower frame potential than their subgroups". Again, it is clear that constructing designs is easier, the more elements one allows for. In general, however, just adding further unitaries to an "almost design" is not going to improve the potential. For group-designs the situation is different, as we now know.

Lastly, statement 7 says that the frame potential of matrix group is "quantized". In that sense, *there are no "approximate group designs"*.

Proof. The equivalence *1.* $\Leftrightarrow$ *2.* $\Leftrightarrow$ *3.* has been established in the discussion preceding the theorem. Claim *4.* is equivalent to *2.*, as $\chi^2 = \chi_S + \chi_A$. The fifth statement follows from a well-known theorem in representation theory (see Ref. [29]). Point *6.* holds true as the number of irreducible components cannot decrease when passing from a subgroup to a supergroup. Claims *7.* and *8.* should be obvious. Lastly, *9.* is valid because for real ζ_U

$$1 = \langle \zeta_U, \zeta_U \rangle = \langle \zeta_U \bar{\zeta}_U, 1_G \rangle = \langle \zeta_{U^{(2)}}, 1_G \rangle,$$

where $1_G : g \mapsto 1$ is the trivial representation. Hence, 1_G is a one-dimensional irreducible component of $U^{(2)}$. But for $d > 2$ we have that $d_s, d_a \neq 1$. □

D. Harvesting character tables

The results of Section III B enable us to identify designs by just looking at character tables of finite groups. Such tables have been the subject to intensive research and are digitally available. We have employed the freely available GAP computer system [32] to search the GAP Character Table Library version 1.1 [33] for unitary designs. Some findings are compiled in Table I. For each dimension d in which a unitary design has been found, one example is included in the table. To access the listed character tables, pass the name to `CharacterTableFromLibrary()`. The column "Irred. character no." gives the position of the design within the list of irreducible characters returned by the `Irr()` -function. E.g., the dialog

```
gap> t:=CharacterTableFromLibrary("J4");;
gap> chr:=Irr(t)[2];;
gap> Degree(chr);
1333
gap> Norm(chr*chr);
2
gap>
```

confirms that the last item in Table I does indeed belong to a unitary group design in dimension 1333.

IV. PHASE SPACE TECHNIQUES

The title *phase space techniques* refers to any method employing the realted concepts of Weyl operators (also known as *generalized Pauli operators*), stabilizer states and the Clifford group. These structures have played a central role in the theory of both spherical and group designs [2, 5, 10, 12, 13]. As the following paragraphs require some rather technical preparations, we state a summary of the results at this point.

In Section IV B *asymptotic* unitary designs will be constructed. By this, we understand a family of sets of unitaries $\mathcal{D}_d$, such that the matrices in $\mathcal{D}_d$ are d-dimensional and $\lim_{d\to\infty} \mathcal{P}(\mathcal{D}_d) = 2$. The intuition behind the construction is as follows: in Section II B, we discussed the relation between the frame potential of operators on $\mathbb{C}^d$ and vectors in $\mathbb{C}^{d^2}$. Hence it is natural to ask whether one can exploit this relation to turn spherical designs into unitary ones. Obviously, in order to obtain *unitary* matrices, we must require the vectors in the spherical design to be maximally entangled. Recall that a maximal set of MUBs is a 2-design and, moreover, that such sets can be chosen to consist of stabilizer states [10]. For bi-partite systems, where each party has prime dimension, it is known that stabilizer states are either maximally entangled or not entangled at all [30]. It is thus reasonable to assume that among the elements of a maximal set of MUBs, there are "enough" maximally entangled ones to yield a set of unitaries with a low frame potential. Fortunately, this intuition turns out to be true and we will find sets of $O(d^4)$ unitaries in dimension $d = p^n$, which approximate a 2-design as $d \to \infty$.

Secondly, in Section IV C, we will revisit the technique of Clifford twirling. Our main contribution to the theory will be a systematical reassessment of what is already known. Indeed, reading the literature, one gets the impression that some confusion has arisen due to the fact that *several distinct Clifford groups exist*. The one used in Refs. [1, 2, 13, 21] is different from the one in Ref. [12]. Going on, we will review a construction by Chau, which meets the Clifford bound in dimensions $2, 3, 5, 7, 11$, and outline a way for circumventing a no-go theorem which asserts that for any other dimension the bound cannot be met. In particular, for $d = 9$, we present a subgroup of the Clifford group which is a 2-design of smaller cardinality than Ref. [12] seems to suggest is possible.

Before presenting these results in detail, the reader must endure the tour-de-force of technical preparations given in Section IV A. It is a peculiarity of the theory to be presented that it works much more smoothly in odd dimensions d than in even ones. While it can be checked that all results in the next section also hold for the qubit case, the proofs are given only for the case of odd d.

A. Introduction

This section contains a very brief outline of the general theory. See Ref. [25, 26] and references therein for a more detailed exposition.

1. Weyl operators, the Jacobi group & the Clifford group

Let us first gather some well-known facts on finite fields [28]. If p is prime and r a positive integer, $\mathbb{F}_{p^m}$ denotes the unique finite field of order p^m. The simplest case occurs for $m = 1$, when $\mathbb{F}_p \simeq \mathbb{Z}_p$, i.e., the set of integers *modulo* p. Now set $d = p^m$ and choose an $r \in \mathbb{N}$. Out of the *base field* $B := \mathbb{F}_d$, one can obtain the fields $\mathbb{F}_{d^r}$ by means of a *field extension*. Extension fields contain the base field as a subset. The extension field possesses the structure of an r-dimensional vector space over the base field. A set of elements of F is a *basis* if it spans the entire field under addition and B-multiplication. The operation

$$\mathrm{Tr}_{F/B}\, f = \sum_{k=0}^{r-1} f^{d^k}$$

takes on values in the base field and is B-linear. Therefore,

$$\langle f, g\rangle \mapsto \mathrm{Tr}_{F/B}(fg)$$

defines a B-bilinear form. For any basis $\{b_i\}$, there exists a *dual basis* $\{b^i\}$ fulfilling the relation $\mathrm{Tr}_{F/B}(b^i b_j) = \delta_{i,j}$ (we do not use Einstein's summation convention). Clearly, if $f \in F$ can be expanded as $f = \sum_i f^i b_i$, with coefficients $f^i \in B$, then duality implies that $f^i = \mathrm{Tr}(f b_i)$.

We will work in the $d := p^m$-dimensional Hilbert space $\mathcal{H} \simeq \mathbb{C}^d$ spanned by the vectors $\{|a\rangle \,|\, a \in \mathbb{F}_d\}$. Define a *character* of $\mathbb{F}_d$ by $\chi_d(a) := \exp(i\frac{2\pi}{p}\mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}(a))$. The relations

$$\hat{x}_d(q)|x\rangle = |x+q\rangle, \qquad \hat{z}_d(p)|x\rangle = \chi_d(px)|x\rangle \qquad (21)$$

define the *shift* and *boost* operators respectively. The Weyl operators (also known as *generalized Pauli operators*) in dimension d are given by

$$w_d(p,q) = \chi_d(-2^{-1}pq)\,\hat{z}_d(p)\hat{x}_d(q), \tag{22}$$

for $p, q \in \mathbb{F}_d$. The phase factors in Eq. (22) have been included to clean up some later formulas. The *phase space* V is defined as $V := \mathbb{F}_d \times \mathbb{F}_d$. We introduce the standard *symplectic inner product* on V by

$$\left[\begin{pmatrix} p \\ q \end{pmatrix}, \begin{pmatrix} p' \\ q' \end{pmatrix}\right] := pq' - qp'. \tag{23}$$

For elements $a = (p,q)^T$ of V, we set $w_d(a) := w_d(p,q)$. Denote by $\mathcal{W}_d := \{w_d(a) \,|\, a \in V\}$ the collection of all Weyl operators. The *commutation relations*

$$w_d(a)w_d(b) = \chi_d([a,b])w_d(b)w_d(a), \tag{24}$$

can be checked to hold.

Let S be a symplectic 2×2 matrix with entries in $\mathbb{F}_d$. There exists a unitary operator $\mu_d(S)$ defined via

$$\mu_d(S)\, w_d(a)\, \mu_d(S)^\dagger = w_d(Sa) \tag{25}$$

for all $a \in V$. We will call $\mu_d(S)$ the *metaplectic representation* of S. Up to phase factors, the set of unitaries of the form $\mu_d(S)\, w_d(a)$ constitute a group, which will be referred to as the *Jacobi group* $\mathcal{J}_d$.

The preceding definition have been made with a single d-dimensional particle in mind. We now consider the situation of n particles, each having $d = p^m$ levels. The Hilbert space becomes $\mathbb{C}^{d^n}$ spanned by $\{|a\rangle \,|\, a \in \mathbb{F}_d^n\}$. Let $p = (p_1, \ldots, p_n), q = (q_1, \ldots, q_n)$. We define the Weyl operators as

$$w_{d,n}(p,q) = w_d(p_1,q_1) \otimes \cdots \otimes w_d(p_n,q_n). \tag{26}$$

In this case, the phase space is set to be $V = \mathbb{F}_d^n \times \mathbb{F}_d^n$ and Eqs. (23,24) continue to make sense if we perceive products between elements of $p, q \in \mathbb{F}_d^n$ as a canonical scalar product: $pq = \sum_i^n p_i q_i$. In complete analogy to the $n = 1$ case, one finds that for any symplectic $2n \times 2n$ matrix S with entries in $\mathbb{F}_d$, there exists an operator $\mu_{d,n}(S)$ such that

$$\mu_{d,n}(S)\, w_{d,n}(a)\, \mu_{d,n}(S)^\dagger = w_{d,n}(Sa) \tag{27}$$

holds for all $a \in V$. Denote the set of Weyl operators according to Eq. (26) by $\mathcal{W}_{d,n}$ and the Jacobi group spanned by $\{w_{d,n}(a)\mu_{d,n}(S)\}_{a,S}$ by $\mathcal{J}_{d,n}$.

For a Hilbert space of prime-power dimension p^s, we can now construct an entire family of different Weyl operators and Jacobi groups. Indeed, for any n, m such that $nm = s$, the Weyl operators $w_{p^m,n}$ are p^s dimensional. Prominent choices include $n = 1, m = s$ (used in Ref. [12]) and $n = s, m = 1$ (used in Refs. [2, 13, 21]). It will turn out that all definitions of the *Weyl operators* coincide, while the various *Jacobi groups* differ. Proposition 7 makes these remarks precise. In order to state it, we need one final definition: the *Clifford group* $\mathcal{C}_{p,n}$ is the set of unitaries mapping the set $\mathcal{W}_{p,n}$ onto itself under conjugation. This definition reflects the general use of word *Clifford group* in quantum information theory [23].

Proposition 7. *Let p^s be a power of a prime. Let $n < n'$ and m, m' be such that $mn = m'n' = s$. Then*

$$\mathcal{W}_{p^m,n} = \mathcal{W}_{p^{m'},n'}, \tag{28}$$
$$\mathcal{J}_{p^m,n} \subset \mathcal{J}_{p^{m'},n'}. \tag{29}$$

The inclusion in Eq. (29) is proper and $\mathcal{J}_{p,s} = \mathcal{C}_{p,s}$.

For the construction in Section IV B, it will be necessary to understand Eq. (28) in more detail. Indeed, it has been realized before [25, 26, 27] that the Weyl operators in $\mathcal{W}_{p^n,1}$ can be written as tensor products of those in $\mathcal{W}_{p,n}$. In what follows, we will refine this picture.

Let $d = p^m$ be a power of a prime, let $B = \mathbb{F}_d$. Let $F = \mathbb{F}_{d^n}$ be an extension field of B. In F, choose a basis $\{b_i\}_{i=1\ldots n}$ over B. Denote the dual basis by $\{b^i\}_i$. Having general relativity conventions in mind, we will adopt the following notation: for an element $f \in F$, we denote its expansion coefficients with respect to b_i by f^i and the coefficients for the dual bases by f_i:

$$f = \sum_i f^i b_i = \sum_i f_i b^i. \tag{30}$$

The Weyl operators in $\mathcal{W}_{d,1}$ act on $\mathcal{H} = \mathbb{C}^{d^n} \simeq (\mathbb{C}^d)^{\otimes n}$, where we choose the isomorphism to be implemented by

$$|q\rangle = |q^1 b_1 + \cdots + q^n b_n\rangle \mapsto |q^1\rangle \otimes \cdots \otimes |q^n\rangle. \tag{31}$$

Lemma 8 (Factoring Weyl operators)**.** *Using the notions introduced above, the Weyl operators in $\mathcal{W}_{d^n,1}$ factor as*

$$w_{d^n}(p,q) = w_d(p_1,q^1) \otimes \cdots \otimes w_d(p_n,q^n). \tag{32}$$

Proof. Denote the common *prime field* $\mathbb{F}_p$ of B and F as P. It is well-known [28] that $\mathrm{Tr}_{B/P} \circ \mathrm{Tr}_{F/B} = \mathrm{Tr}_{F/P}$. Hence

$$\chi_F(pq) \;=\; \chi_B\big(\sum_{i,j} p_j q^i \,\mathrm{Tr}_{F/B}(b_i b^j)\big) = \prod_i \chi_B(p_i q^i).$$

Similarly,

$$\begin{aligned}
\hat{x}_F\big(\sum_i q^i b_i\big)\big|\sum_j x^j b_j\big\rangle &= \big|\sum_i (q^i + x^i) b_i\big\rangle \\
&= \bigotimes_i \hat{x}_B(q^i)|x^i\rangle, \\
\hat{z}_F\big(\sum_i p_i b^i\big)\big|\sum_j x^j b_j\big\rangle &= \prod_i \chi_B(p_i x^i)\big|\sum_j x^j b_j\big\rangle \\
&= \bigotimes_i \hat{z}_B(p_i)|x^i\rangle.
\end{aligned}$$

Using Eq. (22), the claim follows. □

Proof. (of Proposition 7) Eq. (28) follows from the previous lemma. Saying that $\mathcal{J}_{p,r} = \mathcal{C}_{p,r}$ is just rephrasing the definition of the Clifford group. For Eq. (29) the reader is deferred to Refs. [25, 26]. □

2. Stabilizer states

Using the commutation relations Eq. (24) it is immediate that to Weyl operators $w(a), w(b)$ commute if and only if $[a, b] = 0$. Now consider the image of an entire subspace M of V under w:

$$w(M) = \{w(m)|m \in M\}.$$

The latter set consists of commuting operators if for all $m_1, m_2 \in M$, the symplectic inner product vanishes: $[m_1, m_2] = 0$. If that condition is fulfilled, $w(M)$ is called a *stabilizer group*. Consider the operator

$$\rho_M := \sum_{m\in M} w(m)/|M|. \tag{33}$$

One checks that

$$\begin{aligned} \operatorname{tr}\rho_M &= \sum_m \operatorname{tr} w(m)/|M| \\ &= \sum_m d\delta_{m,0}/|M| = d/|M|. \end{aligned} \tag{34}$$

and, using the fact that M is a linear space,

$$\begin{aligned} \rho_M\rho_M &= |M|^{-2}\sum_{m,m'} w(m+m') \\ &= |M|^{-1}\sum_m w(m) = \rho_M. \end{aligned} \tag{35}$$

Hence, if $|M| = d$, then $\rho_M = |\psi_M\rangle\langle\psi_M|$ is a rank-one projector and $|\psi_M\rangle$ is called the *stabilizer state* associated with M. The preceding definition can be extended: choose a character ζ of M (i.e., a function $M \to \mathbb{C}$ such that $\zeta(m_1 + m_2) = \zeta(m_1)\zeta(m_2)$) and set

$$\rho_{M,\zeta} := \sum_m \zeta(m)w(m)/|M|. \tag{36}$$

The calculations Eqns. (34,35) can be repeated and one finds that also $\rho_{M,\zeta}$ projects onto a vector, which will be denoted by $|\psi_{M,\zeta}\rangle$.

3. Mutually unbiased bases

We will recall a well-known construction for MUBs [10]. Once again, let $F = \mathbb{F}_{p^m}$ be a finite field and $V = F^2$ the associated phase space. Let

$$v_a = \begin{pmatrix} a \\ 1 \end{pmatrix}, \qquad M_a = \{\lambda v_a \,|\, a \in F\}. \tag{37}$$

Clearly, M_a is a one-dimensional subspace of V and hence of cardinality $|M_a| = |F| = d$. Because the symplectic form is anti-symmetric $[a, b] = -[b, a]$ it holds for $\lambda v_a, \lambda' v_a \in M_a$ that $[\lambda v_a, \lambda' v_a] = \lambda\lambda'[v_a, v_a] = 0$ and hence the spaces M_a fulfill the requirements of the last section and define stabilizer states. Further, set $\zeta_b^{(a)}(\lambda v_a) := \zeta_b(\lambda) := \exp(i\frac{2\pi}{p}\operatorname{Tr}(b\lambda))$. Each $\zeta_b^{(a)}$ is easily seen to be a character of M_a. Now define the stabilizer states

$$\mathcal{B}_b^{(a)} := d^{-1}\sum_\lambda \zeta_b(\lambda)\, w(\lambda v_a). \tag{38}$$

We claim that these states constitute a set of MUBs. Indeed

$$\begin{aligned} \operatorname{tr}\mathcal{B}_b^{(a)}\mathcal{B}_{b'}^{(a')} &= d^{-2}\sum_{\lambda\lambda'}\zeta_b(\lambda)\zeta_{b'}(\lambda')\operatorname{tr} w(\lambda v_a + \lambda' v_a') \\ &= d^{-1}\sum_{\lambda\lambda'}\zeta_b(\lambda)\zeta_{b'}(\lambda')\delta_{\lambda v_a, \lambda' v_a'} \end{aligned} \tag{39}$$

Now if $a = a'$ then Eq. (39) reduces to

$$\begin{aligned} \operatorname{tr}\mathcal{B}_b^{(a)}\mathcal{B}_{b'}^{(a')} &= d^{-1}\sum_\lambda \exp\big(i\frac{2\pi}{p}\operatorname{Tr}(\lambda(b-b'))\big) \\ &= \delta_{b,b'} \end{aligned} \tag{40}$$

while for $a \neq a'$ we use the property of the finite plane F^2 that the two lines M_a and $M_{a'}$ intersect exactly at $\lambda = 0$ to conclude

$$\operatorname{tr}\mathcal{B}_b^{(a)}\mathcal{B}_{b'}^{(a')} = d^{-1}\zeta_b(0)\zeta_{b'}(0) = d^{-1}. \tag{41}$$

Hence, for a fixed a, the set $\{\mathcal{B}_b^{(a)}\}_b$ forms a basis and all d bases corresponding to different values of a are mutually unbiased. The computational basis corresponds to the set $M_\infty = \{\lambda(1, 0)^T \,|\, \lambda \in F\}$. Repeating the reasoning employed above, one finds that it is unbiased with respect to all the other ones; hence, we have constructed a maximal set of $d + 1$ MUBs.

B. Asymptotic designs from MUBs

This section revolves around the following definition.

Definition 9 (Asymptotic 2-designs)**.** *Let $I \subset \mathbb{N}$ be an index set. A family of sets of unitaries $\mathcal{D}_d$, $d \in I$ is an* asymptotic 2-design *if the matrices in $\mathcal{D}_d$ are d-dimensional and*

$$\lim_{d\to\infty}\mathcal{P}(\mathcal{D}_d) = 2. \tag{42}$$

A priori, it is not clear that this definition has any physical relevance. After all, it is conceivable that, even though the frame potential of $\mathcal{D}_d$ converges, the $\mathcal{D}_d$-twirling channels $T_{\mathcal{D}_d}$ do not become close to the UU-twirling channel in any sensible metric. Indeed, the question of whether asymptotic designs are "almost as good" as strict ones cannot be answered in general, but depends on the application one has in mind. One particular aspect of this question will be illuminated in Lemma 10. We will show that the series of twirling channels $T_{\mathcal{D}_d}$ does converge to T_{UU} in D_{pro}-norm. The latter norm has been defined in Ref. [35], a well-readable account of the merits and perils of different metrics for quantum channels. Specifically, let Λ and Λ' be channels with respective Choi matrices C, C'. If $\Delta = C - C'$, then $D_{\text{pro}}(\Lambda, \Lambda') := d^{-1}\operatorname{tr}|\Delta|$. Some physical interpretations of D_{pro}-convergence are listed in Ref. [35].

Lemma 10. *Let $\mathcal{D}_d$ be an asymptotic 2-design. Then the $\mathcal{D}_d$-twirling channels $T_{\mathcal{D}_d}$ converge to T_{UU} in D_{pro}-norm.*

Proof. Let $C_{\mathcal{D}_d}, C_{UU}$ be the usual Choi matrices, let $\Delta = C_{\mathcal{D}_d} - C_{UU}$. As quantum channels preserve Hermiticity, the Choi matrices and hence Δ are Hermitian. Let $\{\delta_i\}$ be the set of eigenvalues of Δ. By Corollary 3, we know that $\operatorname{tr}|\Delta|^2 \to 0$. Hence, for all i, $|\delta_i| < 1$ eventually and therefore, for large enough d:

$$\begin{aligned} D_{\text{pro}}(\Lambda_d, \Lambda_{UU}) &= d^{-1} \sum_i |\delta_i| < d^{-1} \sum_i |\delta_i|^2 \\ &= d^{-1} ||\Delta||_2^2 \to 0. \end{aligned}$$

□

The technically non-trivial part of this section is contained in the next theorem.

Theorem 11 (Mutually unbiased bases)**.** *Let $d = p^m$ be a power of a prime. Then in $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$ exist $d^2 + 1$ MUBs of which $d^2 - d$ bases are maximally entangled and $d+1$ bases factor.*

Proof. (of Theorem 11) Let $B = \mathbb{F}_d$, $F = \mathbb{F}_{d^2}$. Using the notation of Section IV A 1, we assume that a basis for F over B has been chosen. For $a, b \in F$, let $\mathcal{B}_b^{(a)}$ be a projection onto a stabilizer state in $\mathcal{H}$, as defined in Section IV A 3. Hence

$$\begin{aligned} \mathcal{B}_b^{(a)} &= d^{-2} \sum_{(p,q) \in M_a} \zeta_b^{(a)}(p,q) w_F(p,q) \\ &= d^{-2} \sum_{(p,q) \in M_a} \zeta_b^{(a)}(p,q) w_B(p_1, q^1) \otimes w_B(p_2, q^2). \end{aligned}$$

Defining $N_a = \{(p,q) \in M_a \,|\, p_2 = q^2 = 0\}$, we get

$$\operatorname{tr}_2 \mathcal{B}_b^{(a)} = d^{-1} \sum_{(p,q) \in N_a} \zeta_b^{(a)}(p,q) w_B(p_1, q^1). \quad (43)$$

Clearly, N_a is a B-vector space, so it has cardinality $|N_a| = d^n$ for some n. If $n = 0$, then $\operatorname{tr}_2 \mathcal{B}_b^{(a)}$ equals $\mathbb{1}_1$, so the state was maximally entangled. If $n = 1$, Eq. (43) is of the form of Eq. (36) which makes $\operatorname{tr}_2 \mathcal{B}_b^{(a)}$ a pure state on $\mathbb{C}^d$. Further, $n = 2$ would imply $|N_a| = |M_a|$ and hence $\mathcal{B}_b^{(a)} = \rho_1 \otimes \mathbb{1}_2$ for some density operator ρ_1, which is impossible as $\mathcal{B}_b^{(a)}$ is pure. Lastly, $n > 2 \Rightarrow |N_a| > |M_a|$, which is absurd. Hence any vector in the standard set of MUBs is either a product or else maximally entangled.

Now, $(a\lambda, \lambda) \in N_a$ if and only if $\operatorname{Tr}_{F/B}(a\lambda e^2) = \operatorname{Tr}_{F/B}(\lambda e_2) = 0 \Leftrightarrow \lambda = \lambda_1 e^1 \wedge a\lambda = (a\lambda)^1 e_1$. Assume that

$$a = b \frac{e_1}{e^1} \quad (44)$$

for some $b \in B$. Then $\lambda = \lambda_1 e^1 \Rightarrow \lambda a = \lambda_1 b e_1$ and hence $|N_a| = d$. Conversely, assume that $|N_a| = d$. Then for all $\lambda = \lambda_1 e^1$ we must have that $\lambda a = b e_1$ for some $b \in B$. Solving for a shows that Eq. (44) must hold. Hence among the d^2 bases associated with the sets M_a, there are exactly $|B| = d$ factoring ones. Taking the computational basis into account, the assertion becomes immediate. □

The validity of Theorem 11 implies the existence of asymptotic 2-designs.

Corollary 12 (Existence of asymptotic 2-designs)**.** *Let I be the set of prime-power integers. Then there exists an asymptotic 2-design $\mathcal{D}_d$, for $d \in I$.*

Proof. We compute the frame potential of the $d^2(d^2 - d) = d^4 - d^3$ unitaries $\mathcal{D}_d$ which can be constructed via Eq. (11) from the maximally entangled MUB vectors of Theorem 11:

$$\begin{aligned} \mathcal{P}(\mathcal{D}_d) &= d^4 \sum_{a,a'} \sum_{b,b'} |\langle \psi_b^{(a)} | \psi_{b'}^{(a')} \rangle|^4 / K^2 \\ &= d^4 \left(1 + (d^2 - d - 1) d^{-2}\right) / K \\ &= \frac{2d^4 - (d^{-1} + d^{-2})}{d^4 - d^3} \to 2 \quad (d \to \infty). \end{aligned}$$

□

C. Clifford designs

Let us review the technique employed in Ref. [1, 2, 13] to construct a 2-design. The construction proceeds in two steps. First one realizes that twirling an operator ρ by Weyl matrices reduces ρ to its "Weyl-diagonal" components (see below). Secondly, twirling the resulting operator using the metaplectic unitaries $\mu(S)$ "evens out" the coefficients to yield a $U \otimes U$-invariant state.

Denote by T_W the *Weyl twirl channel* [1, 13]:

$$T_W(\rho) = d^{-2} \sum_{a \in V} w(a) \otimes w(a)\, \rho\, w(a)^\dagger \otimes w(a)^\dagger. \quad (45)$$

Expanding $\rho = \sum_{b,b' \in V} \rho_{b,b'}\, w(b) \otimes w(b')$, we compute:

$$\begin{aligned} &T_W(\rho) \\ &= d^{-2} \sum_{a,b,b'} \rho_{b,b'}\, w(a) w(b) w(a)^\dagger \otimes w(a) w(b') w(a)^\dagger \\ &= d^{-2} \sum_{b,b'} \rho_{b,b'}\, w(b) \otimes w(b') \sum_a \chi(-[b + b', a]) \\ &= \sum_b \rho_{b,-b}\, w(b) \otimes w(-b). \end{aligned} \quad (46)$$

The final transformation follows from the fact that $\chi([b, \cdot\,])$ is a non-trivial character of V for any $b \neq 0$.

The *Clifford twirl channel* [1, 13] is given by

$$\begin{aligned} &T_{\mathcal{C}}(\rho) \\ &= |\mathcal{J}_{\mathbb{F}_p^n}|^{-1} \sum_{U \in \mathcal{J}_{\mathbb{F}_p^n}} (U \otimes U)\, \rho\, (U \otimes U)^\dagger \\ &= |\mathcal{J}_{\mathbb{F}_p^n}|^{-1} \sum_{S \in \mathrm{Sp}(p,n)} (\mu(S) \otimes \mu(S))\, T_W(\rho)\, (\mu(S) \otimes \mu(S))^\dagger, \end{aligned} \quad (47)$$

where $\mathrm{Sp}(p, n)$ denotes the group of symplectic matrices on $V = \mathbb{F}_p^{2n}$. Using the notation and results of Eq. (46), one

concludes:

$$\begin{aligned} &T_C(\rho) \\ &= |\operatorname{Sp}(p,n)|^{-1} \sum_{b\in V} \rho_{b,-b} \sum_{S\in \operatorname{Sp}(p,n)} w(Sb)\otimes w(-Sb) \\ &= \alpha\, \mathbb{1} + \beta \sum_{0\neq b\in V} w(b)\otimes w(-b), \end{aligned} \tag{48}$$

where the constants are given by

$$\alpha = \rho_{0,0}, \qquad \beta = \sum_{0\neq b\in V} \rho_{b,-b}. \tag{49}$$

Eq. (48) follows because the symplectic group acts transitively on $V^\sharp := \{a \in V \,|\, a \neq 0\}$ and hence maps every element of $V^\sharp$ equally often to every other element. It is evident that $T_{\mathcal{C}}$ projects onto exactly two subspaces and is hence equal to T_{UU} by Section III.

Now let G be some subgroup of $\operatorname{Sp}(p,n)$ such that G acts transitively on $V^\sharp$. From the above argument it is clear that $T_{\mu(G)} \circ T_W = T_{UU}$ and hence that $\{w(v)\mu(S) \,|\, v \in V, S \in G\}$ is a unitary 2-design. An obvious choice is to set $G = \operatorname{Sp}(p^n, 1)$ which is the basis of Ref. [12]. The advantage of going from the multi-particle picture to the single-particle picture is an exponential reduction of the cardinality of the design:

$$\begin{aligned} |\operatorname{Sp}(p,n)| &= p^{n^2} \prod_{i=0}^{n-1} (p^{2(n-i)} - 1) \\ &= O(p^{2n^2+n}) = O(d^{2(\log_p d)^2 + \log_p d}), \end{aligned} \tag{50}$$

$$|\operatorname{Sp}(p^n,1)| = p^n(p^{2n}-1) = O(p^{3n}) = O(d^3) \tag{51}$$

(see Ref. [36] for a derivation). What possibilities are there to further improve the cardinality? Clearly, any group acting transitively on $V^\sharp$ must have order $k\,|V^\sharp| = k(d^2-1)$ for some integer k. The smallest value is $k = 1$ and hence $d^2(d^2-1)$ gives a lower bound to the number of elements a Clifford design arising from such a construction can have (c.f. Conjecture 4). In Ref. [12] Chau showed that for $d = 2, 3, 5, 7, 11$, such minimal subgroups do exist. He goes on to rule out the existence of any subgroup G of $\operatorname{Sp}(p^n, 1)$ which has cardinality a multiple of $V^\sharp$. Hence no reduction below $d^2|\operatorname{Sp}(d,1)| = d^5 - d^3$ seems to be possible in general.

However, the argument leaves open the possibility of finding subgroups G of $\operatorname{Sp}(p,n)$ which act transitively on the non-zero elements of the vector space and are smaller than $|\operatorname{Sp}(p^n,1)|$. While we do not know if such groups exist in general, we know of one example for $d = 9$. In Table II we list the generators of a transitively acting subgroup G of $\operatorname{Sp}(3,2)$ of order $160 = 2|V^\sharp|$. It yields a Clifford 2-design of cardinality $2(d^4 - d^2) = 12,960$, where the design induced by $\operatorname{Sp}(9,1)$ has $58,230$ elements and the one associated with $\operatorname{Sp}(3,2)$ consists of $4,199,040$ unitaries. All claims made about the generators can easily be tested by a computer algebra system.

V. MISCELLANEOUS TOPICS

A. Higher orders and general groups

We saw in Section II A that the effect of the twirling channel T induced by some group G and a corresponding unitary representation U_g depends only on the the decomposition of U_g into irreducible constituents (see Appendix VIII A for a version of Eq. (6) valid for general representations).

Based on this observation, the notion of a group design can easily be generalized:

Definition 13 (General group designs)**.** *Let $\mathcal{U}$ be some group of unitary matrices. Then a finite subgroup $\mathcal{D}$ of $\mathcal{U}$ is a $\mathcal{U}$-*group design of order t *if the t-th tensor power of $\mathcal{D}$ has the same number of irreducible constituents as the t-th tensor power of $\mathcal{U}$.*

The most natural setting for applying the above definition is given by unitary designs $\mathcal{U} = U(d)$ of higher order $t > 2$. How many irreducible constituents do we expect the representation $U \mapsto U^{\otimes t}$ to decompose into? The following lemma answers this question by giving the frame potential for unitary t-designs, at least in two special cases.

Lemma 14. *The frame potential of a unitary t-design in dimension d is given by*

$$\begin{cases} t! & \text{for } d \geq t, \\ \sum_{i=0}^{\lfloor n/2 \rfloor} \left(\frac{n!(n-2i+1)}{i!(n-i+1)}\right)^2 & \text{for } d = 2. \end{cases}$$

Once again, we can search the GAP library for examples. Table III gives an example of a matrix group G in $d = 2$, whose 5th tensor power decomposes into 42 irreps, the required value for a 5-design. As a matter of fact, G is very close to being a 6-design: its 6th tensor power has 133 irreducible components, whereas the full unitary group $U(2)$ decomposes into only 132 irreps. Note that the matrices in Table III are not unitary in the standard basis. However, as is well-known [24], any representation of a finite group is equivalent to a unitary one: one can easily construct a similarity transformation mapping the given matrices to unitaries.

Proof. (of Lemma 14) The following facts are well-known [24]: (i) there is a one-one correspondence between irreducible components of the t-th tensor power of $U(d)$ and young frames $\mathcal{F}$ partitioning the integer t into no more than d parts; (ii) the multiplicity of the irrep belonging to a specific frame $\mathcal{F}$ is given by the dimension $d_{\mathcal{F}}$ of the corresponding irrep of S_t.

If $d \geq t$, the restriction "no more than d parts" becomes irrelevant. Using the results of Section III B, we find that the frame potential of a t-design is

$$\sum_{\mathcal{F}} d_{\mathcal{F}}^2 = |S_t| = t!,$$

where the sum is over all young frames with t boxes. The second claim follows in a similar fashion, using well-known formulas for $d_{\mathcal{F}}$ (which can be found, e.g., in Ref. [24]). □

B. Energy-preserving operations as in linear optics

We will briefly comment on a specific representation of the unitary group, which plays a prominent role in linear optics. General references for the introductory paragraphs are Refs. [16, 37, 38, 39]. The most central mathematical object in the description of physical systems of d bosonic modes are the creation and anihilation operators $a_k, a_k^\dagger$. Recall that the set of unitaries on $L^2(\mathbb{R})$ which keep the vector space spanned by the $a_k, a_k^\dagger$ invariant under conjugation form a projective representation of the real symplectic group $Sp(2d)$. The representation is referred to as the *metaplectic representation*. Bosonic systems are often thought about in terms of their *phase space description*, where these metaplectic operations appear in an especially natural way.

The maximal compact subgroup of $Sp(2d)$ is given by the intersection of $Sp(2d)$ with the set of orthogonal transformations $SpO(2d) := Sp(2d) \cap O(2d)$. Physically, the elements of $SpO(2d)$ correspond to energy-preserving or *passive operations*. These operations are exactly the ones which are easily accessible in the laboratory using passive linear optical elements (phase shifts and beam splitters, but no squeezers, which correspond to elements in $Sp(2d)$ which are not contained in $O(2d)$). It is a well-known fact that $SpO(2d) \simeq U(d)$, which might trigger some hope that our theory could be applicable to these systems. However, the metaplectic representation is infinite-dimensional and in this work we did not develop the means to cope with such representations.

In an indirect approach, we can, however, nevertheless exploit the developed formalism: Fortunately, important properties of bosonic quantum states can be described entirely in terms of objects on the $2d$-dimensional phase space. Indeed, define the *canonical coordinates* or quadrature operators $r = (x_1, \ldots, x_d, p_1, \ldots, p_d)$ by

$$x_k := (a_k + a_k^\dagger)2^{-1/2}, \;\; p_k := i(a_k^\dagger - a_k)2^{-1/2}. \tag{52}$$

A much-studied object in particular in quantum optics are the various second moments of the quadrature operators with respect to a given state. Assuming that all first moments vanish, the second moments can be conveniently assembled in a real symmetric $2d \times 2d$ *covariance matrix* γ, defined as

$$\gamma^k{}_l = 2\left(\mathrm{tr}(r_k r_l) + \mathrm{tr}(r_l r_k)\right). \tag{53}$$

An interaction process preserving the energy would then give rise to a map

$$\gamma \mapsto S\gamma S^T =: \gamma', \tag{54}$$

where $S \in SpO(2d)$. The following proposition assures that unitary designs can be used to tackle problems in this context.

Proposition 15 (Averaging over passive operations)**.** *Let $\mathcal{D} \subset U(d)$ be a unitary group design of order t. The image of $\mathcal{D}$ in $SpO(2d)$ under the usual isomorphism is then a $SpO(2d)$-group design of order t.*

A setting that can be studied using designs in this way is the following: consider a system of d interacting bosons. Having a "microcanonical ensemble" in mind, we might be interested in the expected value of various quantities after random energy-preserving interactions have been applied. Haar averages over $SpO(d)$ would constitute a sensible model for such a system (see also Ref. [15]).

Let us give a concrete example. Take $\{|i\rangle\}_i$ as a basis of the vector complex space in which the complex moment matrices are defined. It is straightforward to see that the mean energy of the first mode is given by $E = \langle 1|\Omega\gamma\Omega^\dagger|1\rangle$. The quantity

$$\begin{aligned}\Delta E \;&=\; \int_{U(n)} \langle 1|(U\oplus\bar{U})\Omega\gamma\Omega^\dagger(U\oplus\bar{U})^\dagger|1\rangle^2 dU \\ &-\; \left(\int_{U(n)} \langle 1|(U\oplus\bar{U})\Omega\gamma\Omega^\dagger(U\oplus\bar{U})^\dagger|1\rangle dU\right)^2.\end{aligned} \tag{55}$$

gives the *expected energy fluctuations* of the first mode and is directly amenable to evaluation using unitary 2-designs.

Proof (of Proposition 15). The usual isomorphism between elements $U \in U(d)$ and elements $S \in SpO(2d)$ can be stated as follows: If $U = X + iY$, then S is given by [38, 40]

$$S(U) = \begin{pmatrix} X & Y \\ -Y & X \end{pmatrix}. \tag{56}$$

Setting

$$\Omega = \begin{pmatrix} \mathbb{1} & i\mathbb{1} \\ \mathbb{1} & -i\mathbb{1} \end{pmatrix}/\sqrt{2}, \tag{57}$$

one finds easily that

$$\Omega S(U)\Omega^{-1} = U \oplus \bar{U}. \tag{58}$$

As $\bar{\mathcal{D}}$ is certainly a group t-design if $\mathcal{D}$ is, the statement follows. □

C. Random entanglement

Originally posed by Lubkin and later popularized by Page, the following questions has a long history: what is the average entanglement of a composite system in a pure state [15, 41, 42, 43]. One motivation for studying such problems is to justify the ad hoc "rule of minimal prejudice" employed in statistical physics, which states that among the ensembles compatible with macroscopic observables the one maximizing the entropy is realized in nature. The problem was originally stated in terms of the entropy of entanglement of subsystem A: $S(\rho_A) = -\mathrm{tr}(\rho_A \log \rho_A)$, but various other measures, for example the purity $\mathrm{tr}(\rho_A^2) = ||\rho_A||_2^2$ of ρ_A can be used. The latter quantity has the advantage that its expectation value

$$\int_{U(d)} \| \mathrm{tr}_B[U\rho U^\dagger] \|_2^2 dU \tag{59}$$

is a Haar integral of a second-order polynomial and can thus be directly evaluated by averaging over a 2-design (above, ρ projects onto an arbitrary 2-system state vector $|\psi\rangle$).

Based on this observation, we obtain a simple answer to a special case of this problem as a corollary to Theorem 11 (c.f. Ref. [44] for a much more general, but much longer proof).

Corollary 16 (Average entanglement)**.** *Let d be the power of a prime. The average entanglement of pure states on $\mathbb{C}^d \otimes \mathbb{C}^d$, as measured by the purity, is $2d/(d^2+1)$.*

Proof. We choose $\rho = |0\rangle\langle 0| \otimes |0\rangle\langle 0|$ and average over the Clifford group $\mathcal{J}_{d^2,1}$. The image of $|0\rangle \otimes |0\rangle$ under the action of $\mathcal{J}_{d^2,1}$ constitutes of the bases of Theorem 11. The purity of a reduced density matrix of a product state equals 1, for a maximally entangled state it is d^{-1}. We can thus compute the average by counting:

$$\frac{(d^2-d)d^{-1} + (d+1)}{d^2+1} = \frac{2d}{d^2+1}$$

as claimed. □

Note that, while the question of finding the expected entanglement of a pure state is stated in terms of analysis, we could answer this special case by purely combinatorial means.

VI. SUMMARY

In this work, we presented a first systematic analysis of the mathematical structure of unitary designs. We pointed out a connection to group representation theory, gave bounds on the number of elements of a design, made the relationship to spherical designs explicit, and used this connection to construct approximate unitary designs. Foremost, the pivotal concept of a frame potential has been explored. Intriguingly, the latter quantity appears very naturally in different, seemingly unrelated areas.

While much insight into the structure of unitary designs has been gained, many questions remain unresolved as interesting open problems: finding a systematic way for constructing designs for any choice of parameters t, d or improving the bounds for their cardinalities, to name just two.

VII. ACKNOWLEDGMENTS

The authors thank O. Dahlsten, M. Müller, and A. Serafini for helpful discussions. Support has been provided by the DFG (SPP 1116), the EU (QAP), the EPSRC, the QIP-IRC, Microsoft Research, and the EURYI Award Scheme.

VIII. APPENDIX

A. General twirling channels

Eq. (6) gives an explicit formula for a channel twirling over an *irreducible* representation U_g. In this section, we state the relation for the general case. So assume that $g \mapsto U_g$ decomposes into a set of irreps $U^{(i)}$, which have dimension d_i and occur with multiplicity n_i respectively. The underlying Hilbert space $\mathcal{H}$ then decomposes as

$$\mathcal{H} = \bigoplus_i \mathcal{H}_i \otimes \mathbb{C}^{n_i}, \tag{60}$$

where $\mathcal{H}_i = \mathbb{C}^{d_i}$ (see, e.g., Ref. [24]). The representation U_g itself can be written as

$$U_g = \sum_i U_g^{(i)} \otimes \mathbb{1}_{n_i}. \tag{61}$$

Now set $P_i = \mathbb{1}_{\mathcal{H}_i} \otimes \mathbb{1}_{n_i}$. The twirling channel becomes

$$T_A(\rho) = \sum_i \mathrm{tr}_{\mathcal{H}_i}(P_i'\rho)P_i, \tag{62}$$

as can be checked without difficulty.

[1] C. Dankert (MSc thesis, University of Waterloo, 2005), quant-ph/0512217.
[2] C. Dankert, R. Cleve, J. Emerson, and E. Livine, quant-ph/0606161.
[3] H. Koenig, *Cubature formulas on spheres*, `http://analysis.math.uni-kiel.de/koenig/preprints.html`.
[4] G. Zauner, *Quantendesigns – Grundzüge einer nichtkommutativen Designtheory*, supervised by A. Neumaier (Doctoral thesis, University of Vienna, 1999). Available online at `http://www.mat.univice.ac.at/~neun/papers/physpapers.html`.
[5] J.M. Renes, R. Blume-Kohout, A.J. Scott, and C.M. Caves, J. Math. Phys. **45**, 2171 (2004); D.M. Appleby, quant-ph/0412001.
[6] A. Hayashi, T. Hashimoto, and M. Horibe, Phys. Rev. A **72**, 032325 (2005).
[7] S. Iblisdir and J. Roland, quant-ph/0410237.
[8] A. Klappenecker and M. Rötteler, Proceedings of the IEEE International Symposium on Information Theory, 1740 (2005).
[9] A.J. Scott, quant-ph/0604049.
[10] W.K. Wootters and B.C. Fields, Ann. Phys. **16**, 391 (1989); S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica, **34**, 512 (2002); S. Chaturvedi, Phys. Rev. A **65** 0044301 (2002).
[11] C.A. Fuchs and M. Sasaki, Quant. Info. Comp. **3**, 377 (2003).
[12] H.F. Chau, IEEE Trans. Inf. Theory, **51**, 1451 (2005).
[13] D. DiVincenzo, D.W. Leung, and B.M. Terhal, IEEE Trans. Inf. Theory, **48**, 580 (2002).
[14] G. Tóth and J.J. Garcia-Ripoll, quant-ph/0609052.
[15] A. Serafini, O.C.O. Dahlsten, and M.B. Plenio, quant-ph/0610090. A. Serafini, O.C.O. Dahlsten, D. Gross, and M.B. Plenio, quant-ph/0701051.
[16] J.I. Cirac, J. Eisert, G. Giedke, M. Lewenstein, M.B. Plenio, R.F. Werner, and M.M. Wolf, text book in preparation.
[17] R.F. Werner, Phys. Rev. A **40**, 4277 (1989).
[18] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A. **54**, 3824 (1996).
[19] W. Dür, J.I. Cirac, M. Lewenstein, and D. Bruss, Phys. Rev. A **61**, 062313 (2000).

[20] D. Gottesman, quant-ph/9807006.

[21] W. Dür, M. Hein, J.I. Cirac, and H.-J. Briegel, Phys. Rev. A **72**, 052326 (2005).

[22] E. Hostens, J. Dehaene, and B. De Moor, Phys. Rev. A **71**, 042315 (2005).

[23] Be aware that the Clifford group which appears in the context of quantum information theory [20] has no connection to the Clifford group used e.g. in the representation theory of $SO(n)$ [24].

[24] B. Simon, *Representations of finite and compact groups* (American Mathematical Society, Providence, Rhode Island, 1996); W. Fulton and J. Harris, *Representation Theory* (Springer, New York, 1991).

[25] D. Gross, J. Math. Phys. **47**, 122107 (2006).

[26] D. Gross, diploma thesis (University of Potsdam, 2005). Available at `http://gross.qipc.org`.

[27] A. Pittenger and M. Rubin, J. Phys. A **38**, 6005 (2005) .

[28] D. Jungnickel, *Finite fields* (BI-Wiss.-Verl., Mannheim, 1993).

[29] I.M. Issacs, *Character Theory of Finite Groups* (Academic Press, New York, 1976).

[30] D. Fattal, T.S. Cubitt, Y. Yamamoto, S. Bravyi, and I.L. Chuang, quant-ph/0406168; M. Hein, J. Eisert, and H.J. Briegel, Phys. Rev. A **69**, 062331 (2004); K.M.R. Audenaert and M.B. Plenio, New J. Phys. **7**, 73 (2005).

[31] J.J. Benedetto and M. Fickus, Advances in Computational Mathematics **18**, 357 (2003).

[32] The GAP Group, GAP – Groups, Algorithms, Programming, Version 4.4.7, 2006 (\protect\vrulewidth0pthttp://www.gap-system.org).

[33] T. Breuer. *Manual for the GAP Character Table Library, Version 1.1*. Lehrstuhl D für Mathematik, Rheinisch Westfälische Hochschule, Aachen, Germany, 2004.

[34] V. Dabbaghian-Abdoly, J. Symbolic Comput. **39**, 671 (2005).

[35] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).

[36] B. Huppert, *Endliche Gruppen* (Springer, Berlin, 1967).

[37] P. Kok, W.J. Munro, K. Nemoto, T.C. Ralph, J.P. Dowling, and G.J. Milburn, quant-ph/0512071.

[38] Arvind, B. Dutta, N. Mukunda, and R. Simon, Pramana **45**, 471 (1995).

[39] J. Eisert and M.B. Plenio, Int. J. Quant. Inf. **1**, 479 (2003).

[40] M.M. Wolf, J. Eisert, and M.B. Plenio, Phys. Rev. Lett. **90**, 047904 (2003).

[41] E. Lubkin, J. Math. Phys. **19**, 5 (1978), D.N. Page, Phys. Rev. Lett. **71**, 1291 (1993); S.K. Foong and S. Kanno, Phys. Rev. Lett. **72**, 1148 (1994).

[42] P. Hayden, D.W. Leung, and A. Winter, Comm. Math. Phys. **265**, 95 (2006).

[43] O. Dahlsten and M.B. Plenio, Quant. Inf. Comp. **6**, 527 (2006).

[44] K. Zyczkowski and H.-J. Sommers, J. Phys. A **34**, 7111 (2001).

[45] P.D. Seymour and T. Zaslavsky, Adv. Math. **52**, 213 (1984).

[46] More precisely, Eq. (9) is the *second* frame potential [5], the t-th one being induced by a repulsive force proportional to $\langle\psi_k|\psi_{k'}\rangle^t$. As we will be concerned only with the second potential, we will drop the attribute from now on.

[47] The connection between Eq. (11) and the Jamiołkowski isomorphism Eq. (7) is given by $|v_U\rangle\langle v_U| = d^{-2}\, C_{U\,.\,U^\dagger}$.

[48] Take e.g. $A_{i,j} = |i\rangle\langle j| + |j\rangle\langle i|$, $B_{i,j} = i(|i\rangle\langle j| - |j\rangle\langle i|)$. For $i \neq j$, all operators $A_{i,j}, B_{i,j}$ have the same set of eigenvalues $1, -1, 0, 0, \ldots$ and are thus mutually conjugate. These operators clearly form a basis in the space of trace-less observables.

TABLE I: Some group designs found by the GAP system. The group name and character number refer to the names used by the "ctllib" package [33].

d	K	$K/(d^4-d^2)$	Group	Irred. character no.
2	12	1	7^2:(3x2A4)	10
3	72	1	2^3.L3(2)	2
4	1920	8	2.HSM10	29
5	25920	43.2	2^6:U4(2)	2
6	40320	32	6.L3(4).2_1	49
8	20160	5	4_1.L3(4)	19
9	19440	3	3.3^(1+4):2S5	25
10	190080	19.2	2.M12.2	22
11	13685760	942.	6xU5(2)	3
12	448345497600	21772800	6.Suz	153
13	4585351680	161501.	2.S6(3)	2
14	87360	2.29	Sz(8).3	4
18	50232960	480	3.J3	22
21	9196830720	47397.	3.U6(2)	47
26	17971200	39.	2F4(2)	2
28	145926144000	237714.	2.Ru	37
41	65784756654489600	23294225607.	S8(3)	2
45	10200960	2.49	M23	3
342	460815505920	34.	3.0N	31
1333	86775571046077562880	27483822.	J4	2

TABLE II: Generators of a subgroup G of $\mathrm{Sp}(3,2)$ of order $2(d^2-1)=160$. The group G acts transitively on the non-zero elements of the phase space $V=\mathbb{F}_3^4$ and induces a unitary design, as described in Section IV C.

$$\begin{pmatrix} 2&2&2&0\\ 1&2&2&0\\ 1&2&0&2\\ 0&0&1&1 \end{pmatrix}, \begin{pmatrix} 0&2&1&0\\ 0&0&0&2\\ 1&0&0&2\\ 0&2&0&0 \end{pmatrix}, \begin{pmatrix} 0&2&0&0\\ 2&0&0&0\\ 2&0&0&2\\ 0&1&2&0 \end{pmatrix}, \begin{pmatrix} 0&1&1&0\\ 1&0&0&2\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\ 0&2&0&0\\ 0&0&2&0\\ 0&0&0&1 \end{pmatrix}, \begin{pmatrix} 2&0&0&0\\ 0&2&0&0\\ 0&0&2&0\\ 0&0&0&2 \end{pmatrix}$$

TABLE III: Generators of a matrix group G of order 120. Up to a similarity transformation, the group gives rise to a unitary 5-design with 60 elements. In fact, G is an irreducible representation of $SL(2,\mathbb{F}_5)$ affording the character $X.3$ as listed in the GAP character library [33]. The repersentation has been constructed using the "Repsn" package [34]. Below, $\omega=\exp(\frac{2\pi}{15}i)$.

$$\begin{pmatrix} -1&0\\ 0&-1 \end{pmatrix}, \begin{pmatrix} -\omega^{11}-\omega^{14} & -\omega^{11}-\omega^{14}\\ \omega^{10} & -\omega-\omega^4 \end{pmatrix}, \begin{pmatrix} -\omega-\omega^2-\omega^4-\omega^8-2(\omega^{11}-\omega^{14}) & \omega^6+\omega^9\\ \omega^{11}+\omega^{14} & -\omega^5 \end{pmatrix}$$